APPARATUS AND METHOD FOR DEPOSITING ENCRYPTION KEYS

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an apparatus and a method for depositing encryption keys such as private keys of a public key cryptosystem with depositaries.

2. Description of the Related Art

Confidentiality of information is ensured illustratively by encrypting it with a public key cryptosystem. Such encrypted information cannot be decrypted without recourse to suitable private keys. Where general security of an individual is concerned, no encrypted information belonging to that individual can be decrypted by use of a private key if the individual is for some reason unable to access the system (due to absence, illness, death, etc.). Since the inability to access the system obviously means that any access to the information therein is denied, it no longer matters whether the individual can use his or her private key. Because the information belongs to the individual who owns the private key, there is no need in such a case to make arrangements for any other individual to gain access to the information.

Things are different where corporate security is involved. The unavailability of a private key to any ~~party~~ Party other than the individual who owns it can be a

problem. Individuals working for a company play their respective roles in the organization's activities. Information about corporate activities is necessary for the firm whether or not any such information is encrypted by private keys belonging to specific workers. If encrypted corporate information cannot be decrypted when needed because an individual worker with a private key to the information is out of office, on sick leave or has deceased, an appropriate in-house proxy must be allowed to access the information so that business will proceed unimpaired.

Mechanisms for depositing private keys with depositaries have existed but they have posed the following problems:

1) Whether or not to deposit private keys with depositaries is left to the discretion of the owners of the keys. Of course, rules could be established to stipulate the deposition of private keys, but there is no guarantee that such rules are strictly observed throughout a system. Nor is there any way of verifying whether deposited private keys are legitimate keys.

2) Selection of depositaries is at the discretion of private key owners. Unless a private key is deposited with a competent depositary, the deposited key is unavailable in case of an emergency. A malicious depositary can abuse the entrusted private key.

3) Procedures of deposition are complicated. Generally,

an original private key is divided into a plurality of parts that are stored on a plurality of portable storage media such as floppy disks. The storage media are then deposited with a plurality of depositaries. The procedures are troublesome to both the key owner and the depositaries.

4) Management of entrusted private key parts is left to the discretion of depositaries. Inadequate management by the depositaries can lead to the abuse of a key by an unscrupulous third party.

5) The depositaries designated by a private key owner can conspire to restore and use or abuse the private key without knowledge of the owner. The right of the legitimate key owner can thus be infringed on, and the security of electronic signatures can be compromised.

6) Once a private key is reconstituted, the party or parties that restored the key will permanently possess the same right of access as the original private key owner. This will result in an infringement of the right of the legitimate key owner and compromise the security of electronic signatures.

It is therefore an object of the present invention to overcome the above and other deficiencies of the prior art and to provide an apparatus and a method for implementing a systematically controlled scheme of depositing private keys with depositaries and of sufficiently guaranteeing the security of entrusted

private keys.

SUMMARY OF THE INVENTION

The present invention envisages having encryption keys such as private keys deposited with depositaries in the following manner:

(1) A mechanism is to be established whereby each private key is deposited automatically at the same time that the private key in question and a public key paired therewith are generated.

(2) Rules are to be established whereby depositaries of a given private key are automatically selected.

(3) A mechanism is to be established for the management of deposited keys, wherein the entrusted keys are protected by private keys of depositaries.

(4) Collaborating depositaries may perform only the process requiring the private key they are entrusted with; they cannot acquire the original private key in conspiracy.

(5) There should be a limited period in which to perform the process requiring an original private key.

(6) The process requiring an original private key is limited to the decryption of information that has been encrypted using the private key in question.

In achieving the foregoing and other objects of the present invention and according to one aspect thereof, there is provided an encryption key depositing apparatus

comprising: a unit that generates an encryption key for a user; and a unit that starts a process in response to the generation of the encryption key, the process allowing a depositary deposited with the generated encryption key to store the key in a subsequently recoverable manner.

The structure above controls the deposition of encryption keys in such a manner that the keys are deposited in compliance with system requirements and in a way sufficient to maintain the security of the deposited keys. A selected class of encryption keys instead of all of them may be deposited in the suitably controlled manner. Illustratively, encryption keys may be private keys of a public key cryptosystem. Of course, encryption keys of a routine encryption key system may be deposited.

In a preferred structure according to the present invention, rules may be established to form a basis for determining depositaries. Encryption keys may then be stored in accordance with the established rules.

In another preferred structure according to the present invention, the encryption key depositing apparatus may be implemented as a client-server system wherein recovery information for recovering an encryption key is encrypted by a public key of a depositary and retained in the server. In a further preferred structure according to the present invention,

the server, in response to a recovery request from the depositary, may send to the depositary the recovery information encrypted by the public key of the depositary; wherein the server acquires from the depositary the recovery information decrypted by a private key of the depositary and then encrypted by a public key of the server; wherein the acquired encrypted recovery information is decrypted by use of a private key of the server, the decrypted recovery information being used together with the private key of the server regarding the depositary to decrypt the recovery information about the encryption key; and wherein the decrypted recovery information is used to recover the encryption key. The server may illustratively log historical records of such recovery requests.

In an even further preferred structure according to the present invention, the server, in response to an encryption key acquisition request from the depositary, may encrypt the recovered encryption key using the public key of the depositary and send the encrypted recovered encryption key to the depositary. The server may illustratively log historical records of such encryption key acquisition requests.

In a still further preferred structure according to the present invention, the server may not send the recovered encryption key to the depositary and may perform on behalf of the depositary a process using the

encryption key in response to a processing request from the depositary. The server may illustratively log historical records of such processing requests from the depositary.

Preferably, the historical records may be supplied to the user who owns the encryption key.

It is obvious that the present invention may also be implemented in the form of an encryption key depositing method as well as a computer program product comprising such a method in a manner executable by a computer system.

Other objects, features and advantages of the present invention will become more apparent upon a reading of the following description and appended drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram showing an overall constitution of an embodiment of the present invention;

Fig. 2 is a flowchart of steps constituting a process of the embodiment for establishing rules for depositing private keys;

Fig. 3 is a flowchart of steps constituting a first process of the embodiment for voluntarily determining private key depositaries;

Fig. 4 is a flowchart of steps constituting a second process of the embodiment for voluntarily

determining private key depositaries;

Fig. 5 is a flowchart of steps constituting a process of the embodiment for automatically depositing private keys;

Fig. 6 is a flowchart of steps constituting a process of the embodiment for recovering private keys;

Fig. 7 is a flowchart of steps constituting a process of the embodiment for acquiring private keys;

Fig. 8 is a flowchart of steps constituting a process of the embodiment for using private keys; and

Fig. 9 is a flowchart of steps constituting a process of the embodiment for reporting logs of private key use.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Preferred embodiments of the present invention will now be described in detail with reference to the accompanying drawings.

(1) Selection of private key depositaries (by use of a group hierarchy)

With respect to automated deposition of private keys, the present invention envisages using encryption techniques to prevent illegal access requests from getting fulfilled. However, there are techniques that do not involve encryption in achieving the same objective.

A first process to be carried out is the selection

of depositaries. The depositary refers to an entity with which a private key of an individual is deposited. More specifically, depositaries signify individuals or groups (including assigned roles constituting a group, as has been the case so far) that possess the right to acquire or use private keys they are deposited with. When a group is selected as a depositary for an individual's private key, members making up the group have the right to acquire or use the private key in question.

Typical ways to select depositaries are as follows:

1) Rules are established according to which the entire group hierarchy selects depositaries. For example, an individual belonging to a group may have as depositaries both the person in charge of the group in question and the person in charge of the immediately higher group in the hierarchy, or the person in charge of the group in question and the group in question.

2) Rules are established according to which each group selects its own depositaries.

3) Individual private key owners designate suitable depositaries at their discretion.

If a plurality of depositaries are designated by an individual, it is necessary to specify how many of them need to get together to authorize the right to use the private key deposited by the individual. The number

of depositaries thus specified is called a necessary depositary count.

(2) Selection of private key depositaries (by declaration)

The group hierarchy may not be used in designating depositaries. In such a case, individuals designate appropriate depositaries freely or according to predetermined rules. The designated depositaries are reported to other parties either to gain permission or for compliance checks on depositary designation. The necessary depositary count is specified in the same manner as when the group hierarchy is utilized.

(3) Automatic deposition of private keys

A deposited private key of an individual is encrypted by a public key of a depositary, and the encrypted private key is retained illustratively by a so-called service provider. If there are two or more depositaries for each private key, the deposited private key is divided and the divided parts are each encrypted by a public key. There are known methods for dividing a private key. One such method involves dividing the original private key into three equal parts (called Xp1, Xp2 and Xp3) if there are three depositaries and if the necessary depositary count is two. Three key-part combinations, Xp1 and Xp2, Xp1 and Xp3, and Xp2 and Xp3, are formed and distributed to the three depositaries. Any two of the three depositaries may reconstitute the

original private key when bringing together their deposited key parts.

The deposited private key, owned by an individual, is divided as needed by the owner's client and encrypted thereby using public keys corresponding to the depositaries. The divided key parts are further encrypted by the service provider using public keys. The divided key parts thus encrypted are either retained by the service provider or sent to the depositaries.

(4) Management of deposited private keys

The deposited private keys are encrypted by the depositaries' public keys and managed by the depositaries or by the server.

(5) Acquisition of deposited private keys

Individual depositaries or members of a group depositary may designate a deposited private key and request its use. The designated private key is then decrypted and made available from storage to the requesting depositaries. Alternatively, not the private key itself but the right to use the key in question may be granted. The way in which to provide the right to use the key will be described later.

An original private key is reconstituted (in part or in its entirety) by bringing together the necessary number of encrypted parts of the deposited key from storage. The reconstitution of the private key is carried out either by way of the service provider or

between the individual depositaries involved.

(6) Acquisition of the right to use deposited private keys

Once a private key itself is acquired by depositaries, the key is used freely by these persons or entities. This will compromise the restricted use of private keys by others, which may jeopardize the legitimacy of the public key cryptosystem itself. To prevent such an eventuality, depositaries are barred from acquiring the deposited private key itself and instead allowed only to use it. Specifically, the reconstituted deposited private key is permitted to exist only in the service provider or in the client system. The service provider performs a decrypting process using the private key on behalf of the depositaries.

(7) Preservation of logs of used deposited private keys and subsequent reporting of such key use logs

If a scheme is instituted whereby the right to use deposited private keys is granted by way of the service provider, the service provider keeps logs of decrypting processes it carried out and subsequently reports the logs to the owners of the deposited private keys. The logs contain names of those who requested the uses of private keys, times of day at which the requests were made, target processes (generally decrypting processes only), and target information to be accessed. The reporting is done preferably by electronic mail. It is

also preferred that the logs be reported not only to the private key owners themselves but also to the person in charge of the immediately higher group (i.e., superior). Such measures are effective in preventing access irregularities and discouraging inadvertent acquisition of the right to use deposited private keys.

Below is a description of how this invention is typically embodied.

In the description that follows, specific terms are assigned the following meanings:

[Terms]

target private key: a deposited private key

private key owner: an individual who owns a private key

depositary: an individual with whom a target private key is deposited

deposited private key: information actually sent to a depositary and needed to reconstitute a target private key

depositary count: the number of depositaries allocated to a single target private key

necessary depositary count: the necessary number of depositaries whose deposited private keys are brought together to reconstitute a target private key.

Fig. 1 is a block diagram showing an overall constitution of the embodiment. In Fig. 1, a server 100 and a plurality of clients 200 are interconnected over a network 300. The network 300 links systems together

in the entire corporation and is made up of LANs or LAN segments connected by WAN. The server 100 and clients 200 possess common computer system resources and are configured in a known manner. The configuration of this client-server system is thus of common nature and will not be discussed further. The server 100 has a private secondary storage 101 and a public secondary storage 102, whereas the clients 200 have a private secondary storage 201 each. Information in the private secondary storages 101 and 201 cannot be referenced directly by external entities. Information in the public secondary storage 102 may be accessed freely by external entities but may not be modified thereby.

The private secondary storage 101 of the server 100 includes the server's private keys, recovered private keys, a recovery request log, and a recovered private key use log. The public secondary storage 102 of the server 100 comprises depositary selection rules and a deposited private key list. The private secondary storage 201 of each client 200 contains an individual's pass phrase, an individual's private key, and the server's public key.

In the setup of Fig. 1, the server 100 manages deposited private keys, performs the process of recovering private keys, and logs historical records. Alternatively, these processes may be carried out only by the clients 200.

The embodiment performs the following processes:

(1) Process of establishing rules for private key deposition (see Fig. 2)

This process is performed by the client 200 of an individual in charge of supervising other individuals. Depositaries are controlled in accordance with the established rules. Instead of depositaries being determined according to the private key deposition rules established by this process, the depositaries may alternatively be selected by a first process of voluntarily determining private key depositaries (Fig. 3) or by a second process of voluntarily determining private key depositaries (Fig. 4). Which process to adopt depends on the system requirements.

The process of establishing rules for private key deposition is carried out as follows:

[Step S11] At least one of three candidates is selected: the person in charge of the individual's group, the person in charge of the immediately higher group, and another member of the same individual's group.

[Step S12] The necessary depositary count is specified (at least one and not exceeding the total depositary count).

The rules above are observed in determining the depositaries. Where necessary, the user may make a supplementary choice.

(2) First process of voluntarily determining private key

depositaries (see Fig. 3)

This process is performed by each individual's client 200. If this process is selected, there is no need to retain rules for depositary selection in the server 100 of Fig. 1. Instead, a suitable CA (certificate authority) should be established and supplied with items indicating depositaries in correspondence with public keys. The CA, not shown in Fig. 1, is an ordinary service provider in effect when a public key cryptosystem is employed.

The first process of voluntarily determining private key depositaries is carried out as follows:

[Step S21] At least one individual is designated as a depositary, and a necessary depositary count is specified.

[Step S22] The designated information is automatically sent to the CA to establish correspondence with a public key.

(3) Second process of voluntarily determining private key depositaries (see Fig. 4)

This process is performed by each individual's client 200. If this process is selected, there is no need to retain rules for depositary selection in the server 100 of Fig. 1. Instead, each client 200 must have an area, not shown, for accommodating information indicating that a designated receiver having received a report of the selected depositaries has approved the

choice as appropriate.

The second process of voluntarily determining private key depositaries is carried out as follows:

[Step S31] A report receiver for receiving a report of selected depositaries is designated.

[Step S32] At least one individual is designated as a depositary and a necessary depositary count is specified.

[Step S33] The designated information is reported automatically to the report receiver.

[Step S34] The report receiver evaluates the reported information.

[Step S35] If the report is judged appropriate upon evaluation, the individual's client 200 that originated the report is notified thereof.

[Step S36] A pair of a public key and a private key is generated only if the evaluation is positive.

(4) Process of automatically depositing private keys (see Fig. 5)

This process is performed following the generation of a pair of a public key and a private key by a client 200. Prior to this process, one of three processes above must be carried out: the process of establishing rules for private key deposition (Fig. 2), the first process of voluntarily determining private key depositaries (Fig. 3), or the second process of voluntarily determining private key depositaries (Fig.

4).

The process of automatically depositing private keys is conducted as follows:

[Step S41] A pair of a public key and a private key is generated.

[Step S42] As many deposited private keys as the number of selected depositaries are generated, based on the depositary count and the necessary depositary count.

[Step S43] The deposited private keys are encrypted by use of the depositaries' public keys.

[Step S44] The encrypted deposited private keys are sent to the server 100.

[Step S45] The server 100 records the encrypted deposited private keys.

(5) Process of recovering private keys (see Fig. 6)

This process is performed by the clients 200 of as many individuals as the necessary depositary count, i.e., the necessary number of depositaries whose deposited private keys are to be brought together to reconstitute a target private key. The process of recovering a private key is carried out as follows:

[Step S51] Steps up to step S57 are repeated until the necessary depositary count is fulfilled.

[Step S52] A client 200 presents itself and the private key owner to the server 100.

[Step S53] The server 100 logs the individual who is requesting acquisition of the right to use the private

key as well as the recovery request by the private key owner.

[Step S54] The server 100 returns the deposited private key.

[Step S55] The client 200 decrypts the returned deposited private key using its own private key.

[Step S56] The client 200 encrypts the decrypted deposited private key using a public key of the server 100.

[Step S57] The deposited private key encrypted by the public key of the server 100 is returned to the server 100.

[Step S58] Step S59 is reached if the necessary depositary count is fulfilled.

[Step S59] Using its private key, the server 100 decrypts the deposited private key that was sent from each depositary after being encrypted by the public key of the server 100.

[Step S60] The server 100 puts together the decrypted deposited private keys to recover the original private key.

[Step S61] The server 100 records the time of day at which the original private key is recovered.

[Step S62] Upon elapse of a predetermined time period following the time of day at which the private key was recovered, step S63 is reached.

[Step S63] Upon elapse of the predetermined time

period, the private key is deleted.

(6) Process of acquiring private keys (see Fig. 7)

This process is initiated by an individual depositary wishing to acquire a recovered private key itself. Skipping this process and offering instead a process of only using private keys (Fig. 8) is more effective in preventing illegal use of the private keys and maintaining their reliability.

The process of acquiring private keys is carried out as follows:

[Step S71] The client 200 presents itself and the private key owner to the server 100.

[Step S72] The server 100 checks to see if the target private key is already recovered and present in the server. If the target private key is absent, the process is terminated. If the target key is found to exist, step S73 is reached.

[Step S73] The server 100 checks to see if the individual who is requesting acquisition of the private key is included in a target private key recovery request source log. If the requesting individual is not included in the log, the process is terminated. If the individual is found to be included in the log, step S74 is reached.

[Step S74] The server 100 encrypts the target private key using the requesting individual's public key.

[Step S75] The server 100 sends the encrypted target

private key to the requesting individual.

[Step S76] The client 200 decrypts the encrypted target private key received by use of the requesting individual's private key.

(7) Process of using private keys (see Fig. 8)

This process is initiated by an individual depositary wishing to use a private key. The process illustrates a typical case permitting only the decryption of target information involving a specific private key.

The process of using a private key is carried out as follows:

[Step S81] The client 200 presents itself and the private key owner to the server 100.

[Step S82] The server 100 checks to see whether the target private key is already recovered and present in the server 100. If the target private key is absent, the process is terminated. If the target key is found to exist, step S83 is reached.

[Step S83] The server 100 checks to see whether the individual who is requesting use of the private key is included in the target private key recovery request source log. If the requesting individual is not included in the log, the process is terminated. If the individual is found to be included in the log, step S84 is reached.

[Step S84] The server 100 receives from the requesting

individual the encrypted information desired to be decrypted.

[Step S85] The server 100 records into a recovered private key use log the target information to be decrypted, the time of day at which the decrypting request is issued, the requesting individual, and the private key owner.

[Step S86] The server 100 decrypts the encrypted information using the recovered private key.

[Step S87] The server 100 encrypts the decrypted information using the requesting individual's public key.

[Step S88] The server 100 sends the encrypted information to the requesting individual.

[Step S89] At the client 200, the requesting individual decrypts the information from the server using his or her own private key.

(8) Process of reporting logs of private key uses (see Fig. 9)

This process involves making a subsequent report of recoveries and uses of a private key to its owner. The process is effected automatically when the private key owner gains access to the server 100 for any reason.

The process of reporting logs of private key uses is carried out as follows:

[Step S91] At the client 200, the private key owner accesses the server 100.

[Step S92] The server 100 checks to see whether there exist a recovery request log and a recovered private key use log regarding the private key owner who has accessed the server 100. If no such logs exist, the process is terminated. If the logs are found to exist, step S93 is reached.

[Step S93] The server 100 sends the recovery request log and recovered private key use log to the private key owner.

As described and according to the present invention, a scheme is instituted whereby the deposition of encryption keys is controlled so that the keys are regularly deposited and that the security of the deposited keys is sufficiently guaranteed.

As many apparently different embodiments of the present invention may be made without departing from the spirit and scope thereof, it is to be understood that the present invention is not limited to the specific embodiments thereof except as defined in the appended claims.